

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA,

Plaintiff,

No. CR 16-00440 WHA

v.

YEVGENIY ALEKSANDROVICH  
NIKULIN,

Defendant.

**ORDER RE MOTION FOR  
ACQUITTAL AND MOTION FOR A  
NEW TRIAL**

---

**INTRODUCTION**

A jury convicted defendant of nine counts of computer-related crimes. Defendant now moves for a judgment of acquittal under Rule 29 on all counts or alternatively, for a new trial under Rule 33 on all counts. Both motions are **DENIED**.

**STATEMENT**

After a seven-day trial, a jury convicted defendant Yevgeniy Nikulin of three counts of computer intrusion in violation of 18 U.S.C. § 1030(a)(2); two counts of intentional transmission causing damage to a protected computer in violation of 18 U.S.C. § 1030(a)(5)(A); two counts of aggravated identity theft in violation of 18 U.S.C. § 1028A; one count of conspiracy in violation of 18 U.S.C. § 371; and one count of trafficking in unauthorized devices in violation of 18 U.S.C. § 1029(a)(2).

In short, the background of the case is as follows:

1 In 2012, defendant gained access to the computer of a LinkedIn employee, and used the  
2 employee's credentials to gain access to LinkedIn user credentials. Defendant similarly gained  
3 access to Formspring user credentials by compromising an employee's account. In 2012,  
4 defendant worked with others to sell the Formspring data. Also in 2012, defendant gained  
5 access to a Dropbox employee's account.

6 In arriving at the conclusion that defendant had committed these crimes, the FBI found a  
7 Gmail address (Chinabig01@gmail.com) linked to the above breaches in some capacity. The  
8 Gmail address had been accessed from the same IP addresses used in the LinkedIn and  
9 Dropbox breaches. The Gmail address also created a Formspring account on the same day as  
10 the breach. Additionally, the IP address used in the LinkedIn breach had been accessed by a  
11 gaming account that belonged to defendant. In turn, the gaming account used a different email  
12 address also belonging to defendant. That email address linked to defendant's social media  
13 account. Many of these accounts, including the Chinabig account shared user information,  
14 phrases, and passwords.

15 In October 2016, the grand jury returned an indictment against defendant. Following  
16 extradition from the Czech Republic, a competency evaluation that ultimately found defendant  
17 competent in May 2019, and appointment of new counsel in October 2019, trial ensued on  
18 March 9, 2020, with 12 jurors and four alternates. Trial proceeded until March 11 and was set  
19 to resume on March 17. On March 16, however, six Bay Area counties (including San  
20 Francisco County) issued unexpected shelter-in-place orders due to the COVID-19 pandemic.  
21 As a result, a March 16 order suspended trial for 48 hours. Also on March 16, defendant  
22 moved to continue trial for thirty days given the pandemic. A March 18 order granted the  
23 motion.

24 On April 3, the Court questioned the jurors regarding their availability for an April 13  
25 trial and subsequently filed a summary of their responses. At an April 9 status hearing,  
26 defendant did not move for a mistrial nor a further postponement. Rather, he emphasized his  
27 wish to continue with trial. Given the state of the pandemic and the possibility that there  
28

1 would be an insufficient number of jurors to proceed, an April 9 order postponed trial to May  
2 9.

3 At the end of April, the Court sent questionnaires to jurors to gauge their ability to serve  
4 and filed their responses on April 24. At an April 28 status hearing, defendant did not move  
5 for a mistrial nor a further continuance, but again stated his wish to proceed to trial with the  
6 jury that had been seated in March. Based on the juror responses to the questionnaire and their  
7 COVID-19 concerns, a May 1 order postponed the trial to June 8.

8 At a June 2 status hearing, defendant neither moved for a mistrial nor a further  
9 continuance. The undersigned was open to the possibility of declaring a mistrial, but defendant  
10 wished to proceed with the jury that had been seated in March. At the hearing, trial was  
11 postponed for a final time until July 6. Prior to the resumption of trial, the parties stipulated to  
12 a jury of eleven, ten, nine, eight, seven, or six jurors if good cause existed to excuse the other  
13 jurors.

14 Trial resumed on July 6 with 12 jurors. The jury returned their verdict on July 10,  
15 finding defendant guilty on all counts.

16 True, the undersigned felt at trial at times that the government's case was disjointed and  
17 hard to follow. The government's closing, however, was exceptionally useful and connected  
18 the dots based on the evidence presented at trial in a way that presented a compelling argument  
19 for guilt.

20 Defendant now moves for a judgment of acquittal under Rule 29 as to all counts or  
21 alternatively, for a new trial under Rule 33 as to all counts, arguing the evidence presented  
22 insufficient for a guilty verdict. Defendant has not attacked the structure or postponement of  
23 the trial in any way.

24 **1. RULE 29 MOTION.**

25 Rule 29 provides that a defendant may move for a judgment of acquittal. Under Rule 29,  
26 "[t]he evidence is sufficient to support a conviction if, reviewing the evidence in the light most  
27 favorable to the prosecution, any rational trier of fact could have found the essential elements  
28 of the crime beyond a reasonable doubt." *United States v. Vgeri*, 51 F.3d 876, 879 (9th Cir.

1 1995) (citing *Jackson v. Virginia*, 443 U.S. 307, 319 (1979)). The “evidence is insufficient to  
2 support a verdict where mere speculation, rather than reasonable inference, supports the  
3 government’s case.” *United States v. Nevils*, 598 F.3d 1158, 1167 (9th Cir. 2010) (en banc).

4 **A. SPECIAL AGENT MILLER.**

5 Defendant first argues that Special Agent Jeffery Miller, the only witness to tie the hacks  
6 to defendant, was not credible. For example, although Agent Miller knew of Evgeniy  
7 Bogachev, a Russian man with the same name as defendant and believed to be responsible for  
8 significant computer intrusions, Agent Miller testified that he did not even recognize Bogachev  
9 or know of the specific charges against Bogachev until seeing the FBI “Wanted” poster at trial  
10 (Trial Tr. 693:5–8). Defense counsel, however, cross-examined Agent Miller on these topics,  
11 and he testified that he had he had “followed the evidence” and “at no point during [his] eight-  
12 year investigation did [he] find any ties to Mr. Bogachev” (Trial Tr. 729:13–15).

13 True, the fact that Agent Miller did not conduct a detailed investigation into Bogachev  
14 may have detracted from his credibility. That was for the jury to decide. Even accounting for  
15 that possibility, this order finds that the other evidence presented, including but not limited to  
16 the similarity of usernames and passwords between the Chinabig email account and  
17 defendant’s other personal accounts or the fact that the Chinabig email account searched for  
18 addresses near defendant’s residence, sufficient to sustain a guilty conviction as to all counts.

19 **B. HOTEL VIDEO.**

20 Defendant also argues that the two videos found on Oleksandr Ieremenko’s hard drive —  
21 one of defendant driving a car and another of a hotel conference room meeting — only linked  
22 Nikita Kislitsin and Oleg Tolstikh to the Formspring intrusions, not defendant.

23 On their own, these videos would not be enough for a guilty conviction, but combined  
24 with the other evidence presented at trial such as a photo on Ieremenko’s hard drive showing  
25 defendant in the same car as in the video, the Skype messages between “Evgeniy Lomovich”  
26 and “Sergey Shalyapin,” the emails between Kislitsin, Alexsey Belan, and Mehmet Sozen, as  
27 well as the testimony from the LinkedIn and Formspring witnesses, a guilty conviction as to all  
28 counts can be sustained (Exhs. 21, 22, 66, 76, 120, 152).

**C. MLAT INFORMATION.**

During trial, the government relied on subscriber information obtained from the Russian government through a Mutual Legal Assistance Treaty (MLAT) to identify defendant. The certificate authenticating the subscriber information contained errors. Defendant thus argues the information obtained through the MLAT could not be relied upon because of the nature of the source, the unreliable authentication, and the failure to independently verify the information.

Defense counsel also cross-examined Agent Miller on these topics and he testified that (1) the information came from the Russian government, (2) the certification of authenticity, though incomplete, had a seal of authenticity, and (3) he did not independently verify the information from the MLAT (Trial Tr. 772, 774). The jury heard this testimony and could use that testimony in determining Agent Miller's credibility as well as the reliability of the records obtained from the MLAT. The government presented evidence in addition to the information provided in the MLAT that associated defendant with the data breaches, which the jury could have reasonably used in finding defendant guilty as to all counts.

**D. JAIL CALL.**

Defendant has raised two arguments regarding transcripts of statements he made during jail calls. *First*, he argues the translation of the transcripts did not adequately account for the context of the situation such as his frustration and sense of humor. The government's expert, however, testified on cross examination that the word "vzlomat" sounded like "slomat," which could mean "hack" or "break," and also that meanings of words can change depending on context. The expert also testified that he translated the calls "based on the context presented" (Trial Tr. 404, 407). The jury heard this testimony, and it was up to the jury to determine the reliability of the expert's testimony and of the transcripts. Even ignoring the jail calls in which defendant used the word hack or break, the government presented sufficient evidence for a guilty verdict on all counts.

*Second*, defendant underscores the prejudicial nature of some of these transcripts. The judge is of the opinion that the government should have introduced all but one of these

transcripts, but the Court gave adequate cautionary instructions so as to avert any prejudice to defendant as to the one.

This order recognizes that, as defendant has correctly pointed out, the government presented some evidence that, standing alone, was weak. Importantly, however, defendant does not challenge the evidence itself. Rather, defendant only argues that the government did not present sufficient evidence for the jury to render a guilty verdict. The government, in their closing argument, fairly connected the evidentiary data points in a manner amply sufficient to sustain a guilty conviction. The motion for acquittal as to all counts under Rule 29 is **DENIED**.

## **2. RULE 33 MOTION.**

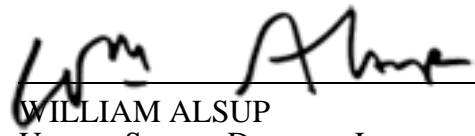
Alternatively, defendant requests a new trial under Rule 33. As with his Rule 29 motion, defendant has only attacked the sufficiency of the evidence, not the evidence itself. Nor has defendant attacked the structure or postponement of the trial in any way. Rule 33 provides that a court “may vacate any judgment and grant a new trial if the interest of justice so requires.” New trials are granted in exceptional circumstances. In particular, even when sufficient evidence exists to sustain a guilty verdict, a new trial may still be granted when “the evidence preponderates sufficiently heavily against the verdict that a serious miscarriage of justice may have occurred.” *United States v. Kellington*, 217 F.3d 1084, 1097 (9th Cir. 2000) (citations omitted).

As stated above, at times, the undersigned found the government’s case disjointed. The government presented weak evidence at times as well, and certain witnesses may not have been wholly credible. Viewing the totality of the evidence in the light most favorable to the government, however, a new trial is not warranted. At trial, the government presented evidence that an individual had stolen data from each of the three victim companies; defendant does not contest this. The government then presented detailed evidence showing how the FBI used certain identifying features from IP addresses, usernames, passwords, email addresses, physical addresses, and website profiles to tie defendant to the crimes. Each of these evidentiary breadcrumbs on their own would not have been enough to present a compelling argument for guilt. Here, however, the closing argument provided a clear explanation as to

1 how the trail of these breadcrumbs, in the context of the timeline of the crimes, ultimately and  
2 powerfully led to the identification of defendant as the individual who committed these crimes.  
3 The remaining weaker evidence did not preponderate “sufficiently heavily” against the verdict.  
4 The motion for a new trial under Rule 33 is thus **DENIED**.

5  
6 **IT IS SO ORDERED.**

7  
8 Dated: October 1, 2020.

9  
10   
11 WILLIAM ALSUP  
12 UNITED STATES DISTRICT JUDGE  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28